Asian Journal of Applied Science and Technology (AJAST)
Volume 6, Issue 4, Pages 40-49, October-December 2022

Methodologies for Resolving Data Security and Privacy Protection Issues in Cloud Computing Technology

Dr. Satinderjeet Singh*

Associate Manager – The Children's Place, 500 Plaza Drive, Secaucus, New Jersey, USA – 07094.
*Email: drsatinderjetsingh@gmail.com**

DOI: https://doi.org/10.38177/ajast.2022.6404

Article Received: 16 August 2022 *Article Accepted: 25 October 2022* *Article Published: 29 November 2022*

ABSTRACT

Because of its accessibility and flexibility, cloud technology is among the most notable innovations in today's world. Having many service platforms, such as GoogleApps by Google, Amazon, Apple, and so on, is well accepted by large enterprises. Distributed cloud computing is a concept for enabling every-time, convenient, on-demand network access to processing resources including servers, storage devices, networks, and services that may be mutually configured. The major security risks for cloud computing as identified by the Cloud security alliance (CSA) have been examined in this study. Also, methods for resolving issues with cloud computing technology's data security and privacy protection were systematically examined.

Keywords: *Cloud technology; Network threats; Data security; Privacy protection issues.*

1. INTRODUCTION

Due to the fact that many corporate security policies, regulations, and processes do not apply to the cloud infrastructure, many security risks arise [1-2]. Even though cloud security has been a focus of study for the past ten years, there are still obstacles needed to be overcome. Investigators, programmers, network operators, and consumers must all have a thorough understanding of the security risks associated with the cloud to take the necessary measures, implement current security protocols, or create new ones [3-5].

1.1. Data Threats

Information is regarded as being among a company's greatest precious resources, and more and more clients are moving their data to the cloud every day. The development, transfer, execution, storage, and deletion of data are all parts of the data life cycle in the cloud. Data may be produced by a client or server in the cloud, transported across the cloud's infrastructure, and preserved there, then the necessary data is moved to the processing area for execution [6]. Data may be completely destroyed by its owner by being erased. Information security is the largest obstacle to attaining cloud computing security.

The main problems with moving data to the cloud are that the consumers are unable to see their data and are unaware of its location [7-8]. They must rely on the service provider to guarantee that infrastructure is secure and that the required security features are implemented to protect their data. Confidentiality, integrity, authorization, availability, and privacy are the information security characteristics that must be upheld in the cloud [9-11].

Nevertheless, the cloud company's inconsiderate management of data is to blame for a lot of data problems. Data breaches, data loss, illegal access, and integrity breaches are among the main dangers in securing data. These problems all regularly affect cloud data. In this paper, we emphasize data breaches and data loss, which CSA lists as the two crucial dangers to cloud computing.

1.2. Network Threats

The network has a significant impact on how well cloud solutions run and interact with clients. Some businesses do not place a high priority on cybersecurity while creating cloud solutions [12]. Lack of cybersecurity opens up attack routes for strangers and malevolent users, posing a variety of network dangers [13-16]. Accounts or service hijacking and denial of service attacks are the two main serious network dangers in the cloud.

1.3. Cloud Environment-specific Threats

The management of the cloud infrastructure is mostly the responsibility of cloud providers. According to a study published by Alert Logic, approximately 50% of cloud customers view service provider problems as a significant danger to cloud computing. Challenges to cloud computing, aside from those posed by service providers, include those posed by hostile cloud users, unsecured interface design and application programming interfaces (APIs), shared technical vulnerabilities, and improper usage of the public cloud.

2. LITERATURE REVIEW

Despite directly receiving them, the investigation was carried out on cloud computing services such as networks, storage, servers, software, and applications. According to research findings, the likelihood of data leakage and other issues has decreased for large systems. On-demand online services are provided through cloud computing. Cloud computing is the ideal option for people who do not want to set up infrastructure in their system if a firm that offers internet services has to invest significant capital funds in infrastructure and issues like machine failure, disc failure, software bugs, etc. This study suggests that cloud users just need to pay for the services they consume rather than spending money on infrastructure.

Researchers have explored the security threats associated with the cloud computing system, its features, the cloud delivery paradigm, and the cloud stakeholders since the cloud's storage of data are expanding quickly, but the safety of open-ended and relatively easily accessible resource is still in doubt. Cloud security was briefly explored by the researchers. These days, more and more individuals use clouds, sending, receiving, and storing sensitive information through networks, making cloud network cybersecurity a key concern. The researchers discuss some of these difficulties. Risk factors that affect cloud security include data corruption, man-in-the-middle attacks, and violation of sensitive data.

Considering clients and servers, the cloud is currently one of the most technologically advanced study areas. Researchers go into detail to make certain that a reputation management solution is used to handle robust security and privacy and to maintain the information-containing transactions table. Virtualization is essential for cloud computing, but its privacy has not received enough attention. This research on cloud security focuses on the impact of virtualization threats on various cloud computing service models. With the aid of virtualization, cloud computing provides a mechanism for the allocation of resources, including applications and infrastructure, and deliberating cloud environments encourage service providers to be adaptable and trustworthy. Cloud security offers a security pattern that cloud service providers must follow. Cloud data is encrypted using the RSA method and a digital signature. To strengthen the privacy of cloud data while it is being moved over networks, security management models, security protocols, and the RSA algorithm with digital signature are described.

The scientific community has discovered that using several cloud providers to handle security has received less emphasis than using a single cloud provider. The focus of this study is on using multiple clouds to lower safety risks and improve information security. Due to the movement of information outside of inter-organizational and internet connectivity, cloud users put the host's control at risk. Researchers give a quick explanation of data security, which has grown to be a major concern for cloud service providers, as well as how to preserve a degree of trust among data owners. Instead of carrying out physical attacks, the miscreants get the choice to harm people's confidential information by committing cybercrime, and it takes time and effort to secure businesses, individuals, and the country in order to avoid these attacks. Data mining and techniques play a significant role in this study's discussion on ensuring the security of cloud data.

The Internet of Things (IoT) and cloud technology are the two most important technologies in modern life. They are anticipated to be licensed and used more, making them the most essential factor of the world wide web. As a result, the focus will be paid to the combination of IoT with cloud computing, known as Cloud IoT. The cloud offers virtual pools of assets to customers via a web interface. These assets encompass architecture, networks, platforms, software, and storage. Since the majority of organizations are trying to migrate their information to the cloud, it is critical to guarantee the security and integrity of cloud consumers' data. This is why it is necessary to discuss the risks associated with data stored in the cloud. The variety of a denial-of-service (DOS) attack and its more significant aspect, distributed denial-of-service (DDOS), are the various kinds of intrusion in cloud computing environments that suggest a technique that is capable of filtering and identifying most struck traffic within a very short amount of time.

One of these main problems is the distributed denial of service attack, which is a type of breach in which several invaders target a single target to stop users of the target network from using its facilities. This attack is characterized by varied methods for detecting and preventing distributed denial of service attacks. In contrast to digital forensics, going to investigate cloud security presents so many difficulties for investigators. For example, when attempting to retrieve evidence from the cloud, forensic investigations may become increasingly challenging. Researchers discussed why cloud complexity impacts digital investigations. The purpose of this study is to discuss different unresolved security risks that impact cloud computing, as well as the benefits and drawbacks of current cloud security measures. Cloud security concerns like data segregation, security, and data integrity are indeed presented.

Cloud is a type of distributed computing where resources and applications are conveyed over the internet and cloud users can pay on a usage basis. Anything that can send data across a network and is linked to the Internet is referred to as the IoT. However, faulty technological implementation and deployment might result in security issues. Researchers discussed the Internet of Things' security concerns and subsequently suggested a security architecture to lessen the vulnerabilities. Cloud computing is a dynamic technique that transforms data and relieves customers of a load of maintaining local storage. Cloud consumers have suggested a technique to ensure security by utilizing stenography and cryptographic methods. Users may easily connect to the network via an internet browser according to the Security-as-a-Service (SaaS) model, which delivers secure communication architecture. The technique is effective since it breaks encryption up into different encryptions. The platforms offer safe access for

different users and complete logical dissociation of data resources and computation related to different organizations. It is constructed by using the OpenStack framework, allowing access to multimodal advancements, and trying to exploit fingerprints is a novel fingerprint method for user authentication. The study explained a cloud computing system that is incorporated and constructed to use software applications and distribute via the internet. Multi-cloud storage serves as one of the essential services in the cloud that is utilized to manage and access cloud data from anywhere.

As per cloud users' suggested new security architecture for cloud framework that provides better secure information processing and protects information from loss, cloud security has emerged as the main issue for cloud experts. This is because unwanted activities are increasing. A self-governing process is necessary to ensure that cloud data is hosted correctly in the cloud server and also that various security methodologies have been mentioned for data storage on the cloud. Data providers and cloud services have unique qualities, and this structure provides data storage and has various security issues. Cloud computing relies on "Utility Computing" and "Software-as-a-Service" to deliver the services that users need; cloud security is a key factor and has many connected challenges and problems. Data privacy, security concerns, and corrupted applications are just a few of the characteristics that have an impact on security. Such problems affect both cloud service providers and customers.

Due to the frequent changes in participation, few studies were able to resolve the difficult problem of data exchange in a multi-proprietor approach using identity privacy and data preservation from an unreliable cloud. For established groups in the cloud, the study presents the Mona secure multi-owner information dissemination structure. Consequently, the user can share data with the network without revealing the cloud's distinctive secret. Additionally, Mona offers quick client cancelation and new client joining. The memory overhead, computation costs, and acceptable security criteria are all met while also guaranteeing efficiency. Huge storage is required for passkey decoding in devices with limited resources, such as smart cards, mobile sensors, and cellphone knobs. For instance, these private passkeys are usually kept in an expensive, tamper-proof memory. This analysis's successes mainly aim to cut down on contact requirements like periodicity and looping connections like composite stamps. To get around this problem, researchers developed a special type of open key encryption called Key Aggregate Cryptosystem (KAC). The classes must conform to a few established hierarchical associations, but the similar attribute displays a consistent size decoding key. The assumption that this control is eliminated is flexible, meaning that no particular connection between the classes is necessary. The criteria model allows for the protection of whole infrastructures.

3. SECURITY TECHNIQUES FOR PROTECTION OF THREATS

In this paper, we outline the adoption of these security measures at several stages to protect clouds against vulnerabilities.

3.1. Data Security

Protection against Data Breaches: To prevent data breaches in the cloud, several security methods and procedures were suggested. One of them is to encrypt data before it is stored in the system and on the cloud.

Effective key management algorithms and cloud-based key security are required for this. Implementing appropriate isolation among virtual machines (VMs) to protect against data leaks, appropriate access controls to restrict access, and performing a risk assessment of the cloud environment to understand where vulnerable data is stored and how it is transmitted between various systems and networks are a few steps to be taken to protect security breaches in the cloud.

3.2. Network Security

Protection against Service Hijacking: By implementing various areas of concern on cloud networks, accounts or service hijacking may be prevented. To identify suspicious attacks, they also use intrusion detection systems (IDS) in the cloud to monitor network traffic and nodes. The effectiveness, interoperability, and virtualization-based environment of the cloud should be taken into consideration while designing intrusion detection and other network security solutions. System-level virtualization and virtual machine monitor (responsible for controlling VMs) approaches were combined to create an IDS system for the cloud. The IDSs in this design are built on virtual machines, and the sensor connections are centered on the widely used IDS Snort. IDS keeps track of the activity and condition of each VM, and its monitoring system allows for instant restarts, stops, and recoveries.

3.3. Security in Cloud Infrastructure

Security against Unprotected Interfaces and APIs - To guard the clouds against the risk posed by unsecured APIs, programmers must build such APIs following trusted platform principles. Additionally, cloud service providers must ensure that every API used in the cloud is developed effectively and is examined for any known vulnerabilities before implementation. To protect information and services from unsecured interfaces and APIs, in addition, it is necessary to build proper authentication procedures and network access. To create safe applications which can aid in preventing these application threats, the Open Web Application Security Project (OWASP) offers guidelines and specifications. Furthermore, while transferring the information to the cloud, clients must review the interface and APIs of cloud service providers.

4. DATA SECURITY AND PRIVACY PROTECTION ISSUES

Comparable to traditional data security and privacy protection, cloud-based data security and privacy protection cover similar ground. Additionally, it participates in each phase of the data life cycle. Since the cloud is open and includes several tenants, its data security and privacy protection policies have unique features. The data life cycle in cloud computing can be seen in Figure 1. The following sections examine challenges with cloud data security and privacy protection related to the data life cycle. The term data life cycle describes the full procedure between data creation till data deletion.

4.1. Data Generation

The ownership of data includes the creation of data. In the conventional IT context, data is often owned and managed by users or organizations. However, it has to be taken into account what to do to retain data ownership if data is to be moved into the cloud. Data owners have a right to understand what personally-identifiable data is being gathered about them, and in certain situations, to terminate such acquisition or use.

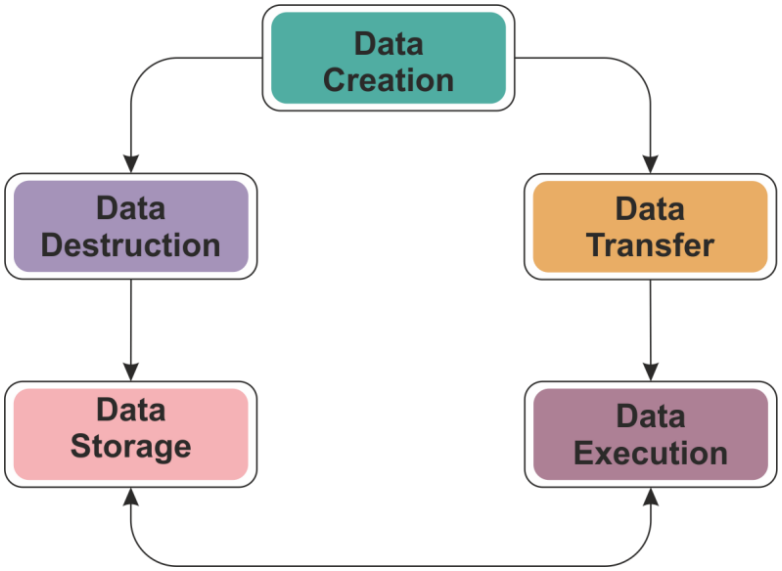

Figure 1. Cloud Computing - Data Life Cycle

4.2. Data Transfer

Data transfer regularly occurs within a firm without security or only with a simple cryptographic technique. For data transmission beyond corporate borders, data confidentiality and integrity must be ensured to avoid information from being accessed and manipulated by unauthorized users. In other words, the encryption process by itself is inadequate. Furthermore, data integrity should be ensured. It must guarantee the employment of transport layer protocols to preserve simultaneously confidentiality and integrity. Confidentiality and integrity of data transmission should be ensured not just from a business and cloud-based storage and also throughout different types of cloud providers. To put it another way, the confidentiality and integrity of the entire data transfer process should be guaranteed.

4.3. Data Use

Data encryption is possible when utilizing a basic storage service like Amazon S3 for static data. Data encryption is frequently not practical for static data in use by cloud-based services in the PaaS or SaaS models. Static data used by cloud-based apps are typically not secured since data encryption will create index and query issues. The data getting handled is essentially not encrypted for every software to operate with, whether it is in a cloud environment or a conventional IT infrastructure. Because cloud computing platforms support many tenants, the information captured by cloud-based apps is kept with the data of other users. Process-related unencrypted data poses a major risk to data security. Situations are more problematic when it comes to the utilization of private data. The proprietors of private data must pay attention to and guarantee that the use of personal information is in line with the data collection's goals and that it is not disclosed to third parties, such as cloud service providers.

4.4. Data Share

Data sharing widens the data's potential applications and complicates data permissions. The owner of the data may grant access to the information to one client, who may then share the data with further parties without the owners' permission. Consequently, while exchanging data, particularly with a third party, the data owners must take into

account if the third party still adheres to the original security protocols and usage limitations. Sharing granularity (all the data or partial data) and data transformation should also be taken into consideration when exchanging private data, concerning data authorization. The granularity of sharing is determined by the content partition granularity and the sharing policies. To isolate critical data from the original data is to alter the information. The information is rendered irrelevant to the data owners as a result of this procedure.

4.5. Data Storage

Two ways to categorize the data in the cloud are (1) data in an IaaS environment, like Amazon's Simple Storage Service, and (2) data in a PaaS or SaaS environment associated with cloud-based applications. Identical to data kept elsewhere, cloud storage requires three components of information security to be taken into account: confidentiality, integrity, and availability. Data encryption is an important means of maintaining data secrecy. The usage of both the encryption algorithm and key strength must be taken into consideration to guarantee the effectiveness of encryption. Computational time must be taken into account since the cloud computing environment involves enormous volumes of data transfer, storage, and management.

4.6. Data Archival

Data archival is concerned with the storage medium, regardless of whether off-site storage is offered, and the length of storage. The danger of data leaks increases if the data are kept on portable media and the media becomes uncontrollable. The integrity of the data will be in danger if the cloud service providers do not offer off-site archiving. Once more, the storage time commensurate with the needs of archives, If not, there may be hazards to the availability or privacy.

4.7. Data Destruction

Whether the data has been destroyed when it is no longer required. The data that was erased may still be present and be recoverable due to the physical properties of the storage media. Sensitive information may unintentionally be disclosed as a consequence of this. By making just little service-related efforts or connecting with a services provider, this may be quickly hosted and subsequently removed. The general public utilizes it to keep their documents for a fair price or without charge. The many kinds of cloud services include Dropbox, Just Cloud, Baidu Container, Google Drive, and others.

Such a setting enables customers to not demand the foundation for various processing services. They can be used to access information from whatever computer is located anywhere in the globe. When related to prior traditional computing techniques, this offers great adaptability by consolidating the elements providing high versatility and multi-occupancy. In this paper, we have examined many factors including cloud security, data sharing, threats, procedures, defensive measures, needs, and societal implications.

5. ISSUES IN CLOUD ENVIRONMENT

The most crucial concern with cloud technology is security. All of it is accommodated on the properties of the providers, which greatly increases the security of the data. It is a significant barrier to the adoption of cloud computing. Security concerns are the top challenge confronting cloud computing, based on an IDC assessment on

the subject. The risks associated with cloud computing include service interruptions, data breaches, privacy invasion, and information destruction. These issues prohibit businesses from utilizing cloud computing services. By using highly-regarded security mechanisms, they could be eliminated. The proportional rise in the number of cybersecurity risks since 2020 is shown in Table 1.

Table 1. Percentages of cybersecurity threats targeted to different industries (2021)

Cybersecurity Threat	Industry		
	Manufacturing (No.)	**Healthcare (%)**	**Financial (%)**
Phishing	1396	29	46
Ransomware	2096	8	5
Trojan	696	46	31
Botnet	496	-	2
Cryptomining	4896	4	5
Others	996	13	11

6. CONCLUSION

As new technology grows and advances, new kinds of cybersecurity dangers appear. Even if it is more vulnerable to some risks than others, cloud computing is not impervious to conventional cybersecurity concerns. The integrity of the data saved on the cloud is just another issue with cloud computing. Numerous places where cloud computing resources are kept may be vulnerable to typical activities that compromise data integrity, like power outages, device malfunctions, or natural disasters. All of these variables might have an impact on the integrity of the data, and if the data is simply saved in the cloud without any additional backups or archiving, the data may be destroyed. Due to the need for redundancies, a lot of individuals and businesses employ a multi-cloud solution, which replicates data among many different cloud service providers. In this paper, the main security threats for cloud computing were looked at. Moreover, methods for resolving issues with cloud computing technology's data security and privacy protection were explored.

Declarations

Source of Funding

This research did not receive any grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The author declares no competing financial, professional, or personal interests.

Consent for publication

The author declares that he/she consented to the publication of this research work.

References

[1] Wu H, Ding Y, Winer C, Yao L. (2010). Network Security for virtual machine in Cloud Computing. In 5th International conference on computer sciences and convergence information technology (ICCIT). DC, USA: IEEE Computer Society Washington, Pages 18–21.

[2] Xiaopeng G, Sumei W, Xianqin C. (2010). VNSS: a Network Security sandbox for virtual Computing environment. In IEEE youth conference on information Computing and telecommunications (YC-ICT). Washington DC, USA: IEEE Computer Society, Pages 395–398.

[3] Popovic K, Hocenski Z. (2010). Cloud Computing Security issues and challenges. In Proceedings of the 33rd International Convention MIPRO. IEEE Computer Society Washington DC, USA, Pages 344–349.

[4] Carlin S, Curran K. (2011). Cloud Computing Security. International Journal of Ambient Computing and Intelligence, 3(1): 38–46.

[5] Bisong A, Rahman S. (2011). An overview of the Security concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1): 30–45. DOI: 10.5121/ijnsa.2011.3103.

[6] Townsend M. (2009). Managing a security program in a cloud computing environment. In Information Security Curriculum Development Conference, Kennesaw, Georgia. NY, USA: ACM New York, Pages 128–133.

[7] Winkler V. (2011). Securing the Cloud: Cloud computer Security techniques and tactics. Waltham, MA: Elsevier Inc.

[8] Ristenpart T, Tromer E, Shacham H, Savage S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA. NY, USA: ACM New York, Pages 199–212.

[9] Zhang Y, Juels A, Reiter MK, Ristenpart T. (2012). Cross-VM side channels and their use to extract private keys. In Proceedings of the 2012 ACM conference on Computer and communications security, New York, NY, USA. NY, USA: ACM New York, Pages 305–316.

[10] Wang Z, Jiang X. (2010). HyperSafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. In Proceedings of the IEEE Symposium on Security and privacy. Washington, DC, USA: IEEE Computer Society, Pages 380–395.

[11] Wang C, Wang Q, Ren K, Lou W. (2009). Ensuring data Storage Security in Cloud Computing. In The 17th International workshop on quality of service. Washington, DC, USA: IEEE Computer Society, Pages 1–9.

[12] Fernandez EB, Yoshioka N, Washizaki H. (2009). Modeling Misuse Patterns. In Proceedings of the 4th Int. Workshop on Dependability Aspects of Data Warehousing and Mining Applications (DAWAM 2009), in conjunction with the 4th Int. Conf. on Availability, Reliability, and Security (ARES 2009), Fukuoka, Japan. Washington, DC, USA: IEEE Computer Society, Pages 566–571.

[13] Santos N, Gummadi KP, Rodrigues R. (2009). Towards Trusted Cloud Computing. In Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, California. CA, USA: USENIX Association Berkeley.

[14] Zhang F, Huang Y, Wang H, Chen H, Zang B. (2008). PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In Trusted Infrastructure Technologies Conference, 2008. APTC'08, Third Asia-Pacific. Washington, DC, USA: IEEE Computer Society, Pages 9–18.

[15] Xiao S, Gong W. (2010). Mobility Can help: protect user identity with dynamic credential. In the Eleventh International Conference on Mobile Data Management (MDM). Washington, DC, USA: IEEE Computer Society, Pages 78–380.

[16] Somani U, Lakhani K, Mundra M. (2010). Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, Pages 211–216.

Cite this article

Satinderjeet, S. Methodologies for Resolving Data Security and Privacy Protection Issues in Cloud Computing Technology. Asian Journal of Applied Science and Technology 6(4), 40–49 (2022).